REMARKS

Applicant requests favorable reconsideration and allowance of this application in view of the foregoing amendments and the following remarks.

Claims 1, 3, 5-17, 19, and 21-23 are pending in this application, with Claims 1, 17, 19, and 22 being independent.

Claims 1, 17, 19, and 22 have been amended. Applicant submits that support for these amendments can be found in the original disclosure at least, for example, in Fig. 6A. Accordingly, Applicant submits that no new matter is being added.

Claims 1, 3, 5-11, 16, 17, 19 and 21-23 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,785,814 to Usami et al. in view of U.S. Patent No. 7,069,584 to Davis. Applicant respectfully traverses this rejection for the reasons discussed below.

As recited in independent Claim 1, the present invention relates to an image processing apparatus that can be used to prevent a counterfeit. Conventionally, it is known to superimpose a tracking pattern on an image to prevent a counterfeit. The tracking pattern may be, for example, information regarding a machine number, user information or the like. However, if such a tracking pattern is superimposed on print data and the position of the tracking pattern is discriminated by a malicious user, the tracking pattern may be tampered with. This leads to deterioration in the reliability of the tracking pattern.

The present invention recited in Claim 1 is directed to address this drawback of the conventional apparatus. The invention recited in that claim includes, *inter alia,* the feature wherein encrypting means encrypts information-added data by randomly arranging additional information together with image data, and wherein the additional information is

randomly arranged across the whole area of the image data. These features make it difficult to detect a position where the additional information is added.

Moreover, by virtue of the above-mentioned features, the present invention recited in Claim 1 renders it difficult for a malicious user to detect, analyze, and/or tamper with the additional information even if blank areas exist where only the additional information occurs and no image exists. This makes it possible to improve the reliability of the image forming apparatus.

Applicant submits that the cited are fails to disclose or suggest at least the above-mentioned features of Claim 1. The Office Action recognizes that Usami et al. does not teach or suggest encrypting the information-added data to make it difficult to detect a position where the additional information is added. Davis is cited to allegedly teach that feature.

Regarding Davis, at page 10 of the Office Action, the Examiner states, "Davis teaches randomly arranging additional information (fig. 2, RANDOM DATA) as well as the image data (fig. 2, SECRET IDENTIFIER) in a process to encrypt (scramble) the data." Applicant respectfully disagrees with the Examiner's interpretation of Davis. In particular, Applicant submits that the "Random Data" mentioned in that document is merely data used for performing encryption (i.e., scrambling), rather than additional data as recited in Claim 1. To the extent the teachings in Davis relate to the claimed features of Claim 1, Applicant submits that the "Secret Identifier" corresponds to the additional information, and the "Super PIN" corresponds to the encrypted additional information.

According to Davis, the space for the Super PIN is provided in a certain area in a chit, and it is easy to locate the area as the space for the Super PIN (see Fig. 2). In addition,

the random arrangement of the Secret Identifier corresponding to the additional information is performed in only the space for the Super PIN, not across the whole area of the chit. This allows the detection, analysis and tampering by a malicious user, since it is easy to locate the area of the Super PIN. Accordingly, since Davis does not provide the features of the present invention recited in Claim 1, Davis cannot provide the benefits arising from the present invention recited in Claim 1.

In summary, the cited art does not recognize the problem addressed by the present invention recited in Claim 1, namely, that a malicious user can tamper with additional information if the position of the additional information is easy to detect, and that cited art does not teach or suggest the above-mentioned features of Claim 1.

Accordingly, even if the teachings of Davis were combined with those of Usami et al., the combination would not disclose or suggest at least the above-mentioned features of the present invention recited in Claim 1.

The other independent claims recite features similar to those of Claim 1 discussed above, and those claims are patentable for reasons similar to Claim 1.

The dependent claims are patentable for at least the same reasons as the independent claims, as well as for the additional features they recite.

In view of the foregoing, Applicant submits that the present invention is in condition for allowance. Favorable reconsideration, withdrawal of the outstanding rejections, and an early Notice of Allowance are requested.

Applicant's undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 530-1010. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

Attorney for Applicant
Brian L. Klock
Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200
BLK/lcw

FCHS_WS 1886299_1.DOC